

METHOD AND APPARATUS FOR DELEGATING DIGITAL SIGNATURES TO A SIGNATURE SERVER

ABSTRACT

One embodiment of the present invention provides a system that facilitates delegating operations involved in providing digital signatures to a signature server. The system operates by receiving a request for a digital signature from a user at the signature server, wherein the request includes an item to be signed on behalf of the user by the signature server. In response to the request, the system looks up a private key for the user at the signature server, and signs the item with the private key. Next, the system returns the signed item to the user, so that the user can send the signed item to the recipient. In one embodiment of the present invention, the system authenticates the user prior to signing the item. In one embodiment of the present invention, the system determines whether the user is authorized to sign the item prior to signing the item.